CORE®

KUNDENAUTHENTIFIZIERUNG IM BARGELDLOSEN ZAHLUNGSVERKEHR

Auswirkungen des neuen RTS (Regulatory Technical Standards) im Kontext PSD II

Holger Friedrich
Dr. Waldemar Grudzien

18. August 2016
COREtechmonitor | Blogpost

Key Facts

- EBA veröffentlicht RTS mit Anforderungen an starke Kundenauthentifizierung und sichere Kommunikation im bargeldlosen Zahlungsverkehr
- Wesentliche Inhalte betreffen die Regelung der starken Kundenauthentifizierung inklusive Ausnahmeregelungen, den Einsatz von Biometrie sowie Klarstellungen zu Aspekten wie Kanaltrennung und Risikoanalysen
- Anforderungen haben vielfältige Auswirkungen auf Sicherheit, Prozesse und Geschäftspotenziale von Finanzinstituten

Report

1. Rationale

Der Regulator dringt in diversen Initiativen darauf, dass Finanzinstitute Dritten Zugang zu Daten und Informationen schaffen, deren Abschottung nicht zu rechtfertigen ist. Diese durch die Payment Service Direktive PSD II forcierte Marktöffnung der Finanzindustrie wird durch den jüngst veröffentlichten „RTS“ (Regulatory Technical Standards) der EBA in zwei wichtigen Punkten spezifiziert: der starken Kundenauthentifizierung und der sicheren Kommunikation bei elektronischen Zahlungsdiensten. Diese Regelungen haben hohe Auswirkungen auf bestehende Standards und etablierte Prozesse im bargeldlosen Zahlungsverkehr.

Das Dokument besteht aus den zwei Hauptteilen „Hintergrund und Rationale“ im Kapitel 3 sowie aus Kapitel 4 mit 23 Artikeln, die später als finale Version den eigentlichen RTS darstellen werden. Zwar werden final nur die Artikel als RTS verbindlich sein, jedoch bezieht die EBA im 3. Kapitel sehr wohl Stellung zu einzelnen Aspekten und legt sich auf eine Meinung fest. Es bleibt abzuwarten, welche Auffassungen der EBA sich letztlich in einzelnen Artikeln des RTS finden.

Mit der folgenden Darstellung geben wir einen Überblick über die wesentlichen Inhalte und Auswirkungen aus dem RTS der PSD II. Auf die analysierten Textstellen wird referenziert.

2. Analyse

2.1 Rahmen

Die PSD II gibt vor, dass die bisher über interne APIs genutzten, bankeigenen Dienste in der bilateralen Beziehung zum Kunden bis Januar 2018 über öffentliche Schnittstellen Dritten zur Verfügung gestellt werden müssen. Sie ist seit dem 12. Januar 2016 in Kraft und ab dem 13. Januar 2018 anzuwenden. Die PSD II überträgt 11 Mandate an die europäische Bankenaufsicht EBA, einzelne Aspekte des Zahlungsverkehrs zu spezifizieren. Die EBA hat am 12. August 2016 das Konsultationspapier mit den Anforderungen an starke Kundenauthentifizierung und sichere Kommunikation bei elektronischen Zahlungsdiensten veröffentlicht –RTS specifying the requirements on strong customer authentication (SCA) and common secure communication under PSD II.

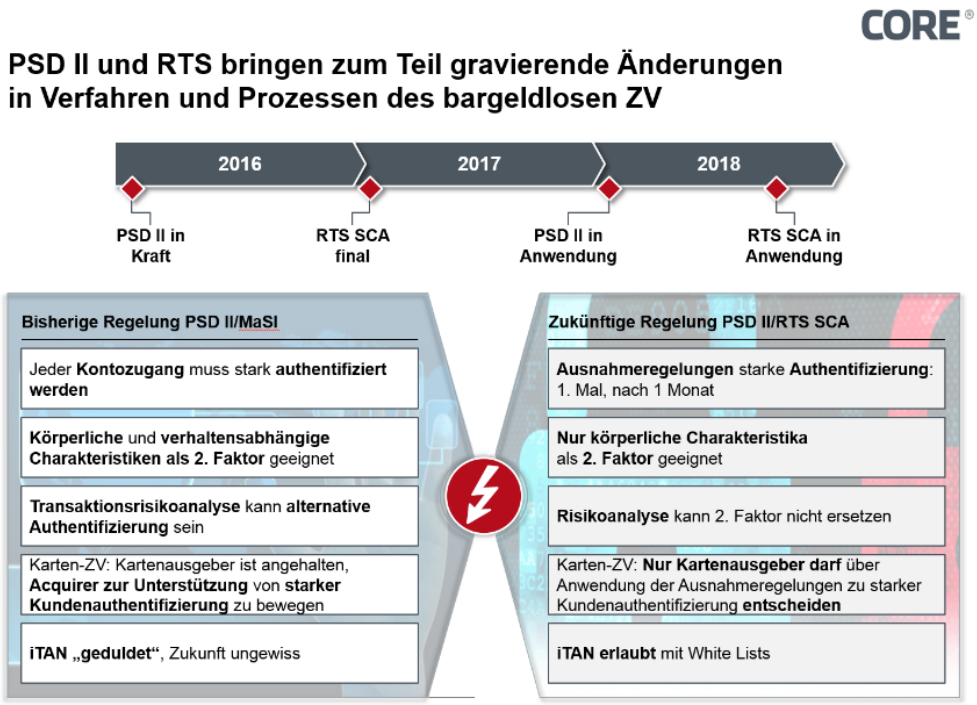

Abbildung 1: Wesentliche Änderungen durch PSD II i.V.m. RTS SCA gegenüber Situation heute

Das vorliegende Konsultationspapier stellt die Umsetzung des Mandats aus PSD II Artikel 98 (Regulatory technical Standards on authentication and communication) dar. Die veröffentlichte Version basiert auf dem am 8. Dezember 2015 veröffentlichten Diskussionspapier, in das Kommentierungen von 118 Einsendern integriert wurden.

Die Konsultationsphase für den RTS endet am 12. Oktober 2016, danach wird die EBA den finalen RTS spätestens zum 12. Januar 2017 veröffentlichen. Da nach der PSD II der RTS binnen 18 Monaten nach Annahme der EU-Kommission durch die Marktteilnehmer angewendet werden muss, haben diese mindestens bis Oktober 2018 Zeit, die Anforderungen umzusetzen.

Die Detailregelungen des RTS werden hohe Auswirkungen auf bestehende Standards und etablierte Prozesse im bargeldlosen Zahlungsverkehr haben, etwa bei der (Nicht-) Anwendung von starker Kundenauthentifizierung im Kontozugang und zur Zahlungsinitiierung oder bei der Nutzung von risikobasierten Analysen.

Der RTS adressiert folgende Aspekte bei Zahlungsdiensteanbietern:

- Starke Kundenauthentifizierung beim Zugang zum Konto, bei der Zahlungsauslösung und bei jeglicher Aktion über Fernzugriff (remote channel), die zu einem Geldverlust oder sonstigem Missbrauch führen kann.
- Ausnahmen bei der Anwendung von starker Kundenauthentifizierung und von Sicherheitsmaßnahmen zum Schutz der geheimen Sicherheitsdaten des Zahlungsdienstenutzers wie PIN und TAN.
- Maßnahmen zum Schutz der geheimen Sicherheitsdaten.
- Anforderungen an eine einheitliche, sichere und offene Kommunikationsschnittstelle zwischen kontoführender Stelle (ASPSP), Zahlungsauslöse

diensten (PISP), Kontoinformationsdiensten (AISP), kartenausgebenden Zahlungsdiensteanbietern (PIISP), Zahlern, Zahlungsempfängern und weiteren Zahlungsdiensteanbietern.

2.2 Details

Ein Lösungsansatz für die beschriebene Herausforderung besteht in der Umstrukturierung bzw. Erweiterung der bestehenden Wertschöpfung um eine zentrale digitale Plattform, welche als Ausgangsbasis und Anknüpfungspunkt für mobilitätsassoziierte Angebote im weitesten Sinne dienen kann.

Das Erfolgspotenzial der disruptiven Unternehmen der letzten Jahre ist evident: Innovative Unternehmen wie Alibaba, Facebook, Uber und Airbnb konnten innerhalb kürzester Zeit beachtliches Wachstum generieren Die innovativen Konzepte sind durch fünf Grundelemente gekennzeichnet:

Zur Errechnung des Authentikationscodes (für Kontozugang oder zur Zahlungsinitiierung) nach Artikel 1 fließen die nach EBA als stark anerkannten drei Elemente Wissen, Besitz und Inhärenz (biometrische Charakteristiken) ein. Keins dieser Elemente darf aus dem Authentifikationscode zurückgerechnet werden können. Weiterhin nennt Artikel 1 Mechanismen der starken Kundenauthentifizierung, welche vor allem die kontoführende Stelle teilweise vor Herausforderungen stellen dürften. So sollen nach Artikel 1 Nr. 3(e) zur Verhinderung, Detektion und zum Stoppen von betrügerischen Transaktionen in der Banking-Sitzung Infektionen mit Schadsoftware erkannt und bereits bekannte Schadensszenarien (ii.) einbezogen werden. Hier bleibt abzuwarten, was die EBA im Detail erwartet. Soll ein Zahlungsdiensteanbieter eine Infektion des privaten Kunden-Rechners erkennen? Was soll die Bank im Positiv-Fall unternehmen? Nur die Transaktion stoppen oder auch den Kunden kontaktieren und für die Bereinigung des Rechners sorgen? Auch die Anforderung nach Informationen zum verwendeten Kundengerät (iv.) müssen mit mehr Details versehen werden. Wird darunter nur das durch eine Bank ausgegebene Gerät verstanden wie ein TAN-Generator oder fällt hierunter auch das private Smartphone des Nutzers? Fragen dürfte auch die geforderte Berücksichtigung des Risikoprofils des Nutzers und seines Endgerätes (v.) aufwerfen. Nach welchen Kriterien und Schwellen darf oder muss eine kontoführende Stelle einem Nutzer seine gewollte Transaktion verweigern? Maßnahmen wie der Einbezug von gesperrten Bankkarten (i.) und der Zahlungshistorie des Nutzers (iii.) in die Risikoanalyse können dann wiederum als „bekannt“ eingestuft werden.

Artikel 2 enthält eine Klarstellung zur im DK-Jargon genannten „Kanaltrennung“; demnach dürfen bei gegebener Unabhängigkeit/Trennung von Kanal, Endgerät oder Apps Zahlungsvorbereitung und Zahlungsinitiierung auf einem Endgerät erfolgen.

Eine elementare Abweichung von der Regelung der PSD II zum Kontozugang (PSD II Artikel 97(1)) stellt der RTS in Artikel 8 bei den Ausnahmen der Anwendung der starken Kundenauthentifizierung auf: Muss nach PSD II jeder Kontozugang stark authentifiziert werden, so muss nach dem RTS der erstmalige Kontozugang und der erste Kontozugang nach Ablauf der Zeitspanne von einem Monat, in dem der Kontozugang ohne starke Kundenauthentifizierung gewährt wurde, wieder stark authentifiziert werden.

Einerseits stellt diese Vereinfachung eine Konzession an diejenigen Länder dar, die schon immer überwiegend mit statischer Kundenauthentifizierung arbeiten – wie

Deutschland. Andererseits birgt diese Regelung ein starkes Potenzial der Kundenverwirrung, da dieser nun mal stark und meistens nicht stark authentifiziert werden muss. Hier wird es spannend zu beobachten, wie sich die kontoführenden Institute im Markt entscheiden werden; aus Gründen der Convenience könnte hier einiges für den permanenten, stark authentifizierten Kontozugang sprechen. Zum anderen stellt diese Regelung sicherlich eine Konzession der EBA an die Europäische Kommission als Wettbewerbsbehörde dar, die Kontoinformationsdienste schützen will. Auch hier bleibt abzuwarten, wie sich europäische und nationale Wettbewerbshüter verhalten werden, sollten Banken aus den oben genannten Convenience-Gründen beim Kontozugang ausnahmslos auf starke Authentifizierung setzen.

Weiterhin erwähnenswert zum Artikel 8 sind die Betragsgrenzen bei kontaktlosen Kartenzahlungen am PoS von 50 Euro für Einzeltransaktionen und 150 Euro als Maximalbetrag für eine Serie nicht stark authentifizierter Kartentransaktionen. Damit wird die bisher im Markt vorherrschende Grenze von 30 Euro pro Kartentransaktion signifikant angehoben.

Sehr interessant ist ferner die Ausnahmeregelung für Zahlungsinitiierungen bei Einsatz von White Lists der Zahlungsempfänger nach Artikel 8 Nr. 2. Da hier keine starke Authentifizierung des Kunden mehr vorgeschrieben ist, könnten Banken aus Gründen

der Kundengewöhnung weiterhin auch die iTAN als Legitimationsmittel einsetzen, die – nach Ansicht der Autoren völlig zu Unrecht – als nicht mehr sicher genug eingeschätzt wird.

Zur Biometrie äußert sich die EBA dahingehend (Rationale Nr. 29), dass sie verhaltensabhängige Charakteristiken nicht als alleinigen 2. Faktor anerkennt. Gleichwohl dürfen diese Charakteristiken als ein Element in Risikoanalysen zur Schadensprävention einfließen. Unter verhaltensabhängige biometrische Charakteristiken fallen zum Beispiel Tippverhalten, Gang oder auch Bewegungsmuster der Computermaus. Demgegenüber sieht die EBA demnach die körperlichen Charakteristiken als sicher genug für einen alleinigen 2. Faktor an, sodass beispielsweise das im Banking bereits breit eingesetzte Fingerabdruckverfahren weiterhin als 2. Faktor zum Kontozugang wie auch zur Zahlungsauslösung eingesetzt werden kann. Weitere, im Banking gut nutzbare körperliche Charakteristiken sind Gesicht, Augen, Stimme und Venen (Handfläche, Finger). Des Weiteren bedarf die Aussage in Artikel 5 zur Bereitstellung von Geräten und Software einer Konkretisierung, denn meistens liefern nicht Zahlungsdiensteanbieter Geräte mit biometrischen Sensoren, sondern Telekommunikationsunternehmen oder im weitesten Sinne Technologieanbieter. Weder der RTS noch die PSD II wird diese Zulieferer von Kundenendgeräten in die Regulierung einbeziehen, somit verbleibt die Verantwortung für sichere Biometrie letztendlich beim Kreditinstitut.

Nach Rationale Nr. 41 darf im Karten-Zahlungsverkehr über das Internet nur noch der

Kartenausgeber über Anwendung der Ausnahmeregelungen zu starker Kundenauthentifizierung entscheiden. Bei der MaSI wird der Kartenausgeber angehalten, den Kartenakzeptanten (Händler) zur Unterstützung von starker Kundenauthentifizierung zu bewegen. Nun liegt die Entscheidung alleine beim

Kartenausgeber. Dies erhöht die Sicherheit im Gesamtsystem Karten-Zahlungsverkehr im Internet.

Zur sicheren Kommunikation zwischen kontoführender Bank und den drei durch die PSD II eingeführten Marktteilnehmern Zahlungsauslösedienst (PISP), Kontoinformationsdienst (AISP) und kartenausgebende Zahlungsdiensteanbieter (PIISP) müssen kontoführende Banken eine Schnittstelle bereitstellen (Artikel 19 Nr. 1). Diese muss die Identifizierung der drei Teilnehmer (Artikel 19 Nr. 1(a)) sowie deren drei Grundservices (Artikel 19 Nr. 1(b)) unterstützen. Weitere zum Teil fein granulierte Details werden durch Artikel 19 vorgegeben. Zum Beispiel muss die Schnittstelle die gleichen Funktionen und Servicequalitäten zur Verfügung stellen, wie sie der Kunde im direkten Aufruf im Online-Banking erfährt (Artikel 19 Nr. 6). Auch muss die Schnittstelle über Testmöglichkeiten für die drei Zahlungsdiensteanbieter verfügen (Artikel 19 Nr. 7). Insgesamt sind die Anforderungen an die allein auf Kosten der Kreditinstitute einzurichtende Schnittstelle generisch aber herausfordernd, da sie den gleichen Service Level (z.B. Verfügbarkeit, Sicherheit) gewährleisten muss wie das Onlinebanking.

Nach Rationale Nr. 69g sollen Konteninformationsdienste so oft auf die Konten zugreifen dürfen, wie es der Zahlungsdienstenutzer wünscht, und im Falle der Inaktivität des Nutzers maximal zwei Mal pro Tag. Diese Regelung darf als Entgegenkommen für die kontoführenden Stellen verstanden werden, um deren IT-Infrastrukturen zu entlasten.

Zum Outsourcing von IT-Dienstleistungen durch Zahlungsdiensteanbieter unterstreicht der RTS in Rationale Nr. 79 und Nr. 80 die Aussagen der PSD II, wonach durch Outsourcing keine negativen Folgen hinsichtlich Betrieb, Sicherheit, Monitoring und Aufsichtsfähigkeit entstehen dürfen. Zahlungsdiensteanbieter bleiben demnach voll verantwortlich für ihre Auslagerungen; diese Sicht des RTS entspricht voll und ganz der Auffassung der nationalen Aufsicht, denn nach BaFin ist das IT-Outsourcing ein normaler Anwendungsfall (reguliert durch §25b Kreditwesengesetz KWG und Allgemeiner Teil AT 9 der MaRisk).

3. Schluss

Es zeigt sich, dass der Regulator über die Regelungen der PSD II sein Ziel der Marktöffnung durch Schaffung eines Kontozugangs für Dritte erreichen wird. Mit Hilfe der Konkretisierungen im vorliegenden RTS soll der Kontozugang sicher für Kunden, Banken und Dritte umgesetzt werden können. Hier müssen erstens die im Text angedeuteten Reaktionen im Markt sowie zweitens die möglichen Gegenreaktionen der Wettbewerbs- und Aufsichtsbehörden abgewartet werden, und drittens muss auch abgewartet werden, wie sich die gegen Bankkunden gerichtete Kriminalität weiterentwickeln wird.

Heute, d.h. im bilateralen Verhältnis Kunde-Bank sind die Angriffsvektoren und Schadensmuster weitestgehend „ausentwickelt“ und werden nur noch reaktiv fortentwickelt. Mit der PSD II wird das bilaterale Verhältnis um eine dritte Partei geöffnet. Die Angriffs- und Schadensmöglichkeiten werden sich, wie in jedem IT-System, das so gewaltig erweitert wird, potenzieren. Erst dann lässt sich beurteilen, ob der RTS sein Ziel der sicheren Zahlungsdienste erreicht hat. Auf jeden Fall hat diese Regulierung neben der Marktöffnung auch hohe Auswirkungen auf bestehende Sicherheitsstandards und etablierte Prozesse bei den kontoführenden Banken;

angefangen bei der einzurichtenden Schnittstelle über neue Risikomodelle bis hin zu sich bietenden Geschäftsopportunitäten durch den Kontozugang für die Banken – die diese aber auch zu nutzen verstehen müssen.

Sources

INTERNET:

EBA, 2016

https://www.eba.europa.eu/-/eba-consults-on-strong-customer-authentication-and-secure-communications-under-psd2

Holger Friedrich ist Managing Director bei CORE. Er verfügt über 20 Jahre Beratungserfahrung im Bankensektor, wo er u.a. die Leitung der Planung und Implementierung der IT-Ziellandschaft bei der Fusion zweier Banken übernahm. Zuletzt verantwortete er die Konzeption eines IT-Programms im Großkundengeschäft zur Ablösung verschiedener Investment-Banking-Systeme durch eine moderne OTC-Plattform.

Mail: holger.friedrich@coretransform.com

Dr. Waldemar Grudzien ist Transformation Engineer bei CORE und verfügt über langjährige Erfahrung in einem nationalen Verband des Finanzsektors, wo er den Bereich Retail Banking und Banktechnologie verantwortete. Dabei fokussierte er sich hauptsächlich auf die Sicherheitsregulierungen der Finanzindustrie und deren technologische Auswirkungen auf IT-Infrastrukturen.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 16344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk